Codify
BY AAPC

Health Information Compliance Alert

Case Study: Implementing New Technology? Perform A Risk Analysis Or Pay The Price

Don't let portable devices go without proper encryption and proper security precautions.

If you allow employees to use web-based document sharing applications without thoroughly evaluating the risks, you're leaving your organization wide open to a HIPAA violation and a breach incident. Learn from these most important lessons in the latest breach case.

On July 10, the **HHS Office for Civil Rights** (OCR) announced that **St. Elizabeth's Medical Center** (SEMC) has agreed to settle potential HIPAA violations by paying out $218,400 and adopting a corrective action plan (CAP). SEMC provides inpatient and outpatient tertiary care services in Brighton, Mass.

Beware of Using Internet Applications

Part of the settlement agreement stems from an OCR complaint back in 2012 alleging that SEMC staff members were using an Internet-based document sharing application to store documents containing electronic protected health information (ePHI). OCR's investigation determined that SEMC failed to perform a risk analysis before beginning use of the application.

"Organizations must pay particular attention to HIPAA's requirements when using Internet-based document sharing applications," warned OCR Director **Jocelyn Samuels** in a July 10 statement. "In order to reduce potential risks and vulnerabilities, all workforce members must follow all policies and procedures, and entities must ensure that incidents are reported and mitigated in a timely manner."

Important: One key takeaway here is to ensure that your organization's HIPAA policies and procedures "address the use of Internet-based applications, including document and file-sharing applications," advised attorneys **Elizabeth Hodge** and **Thomas Range** in a July 15 analysis for **Akerman LLP**.

Perform a Risk Analysis Before Using New Tech

But the web-based document sharing application wasn't itself the only problem the big problem here was that SEMC didn't perform a risk analysis prior to using the application. Under HIPAA, covered entities (CEs) "are required to implement and periodically review administrative, physical and technical safeguards to protect the security of the ePHI that they create, transmit, receive, store or maintain," wrote attorneys **Laurie Cohen**, **Valerie Montague** and **Brooke Lane** in a July 24 analysis for **Nixon Peabody LLP**.

"Risk assessments are intended to identify and correct potential vulnerabilities in security procedures and systems," the Nixon Peabody attorneys stated. And in light of heightened scrutiny of CEs and their business associates (BAs) by OCR, all organizations that handle PHI should evaluate their HIPAA compliance plans, including security systems and procedures.

Bottom line: This case offers the lesson that you should perform a risk analysis before using new technologies, according to **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems LLC** in

Charlotte, VT. You can use OCR's security risk assessment tool to get started on your risk analysis: www.healthit.gov/providers-professionals/security-risk-assessment.

Train Your Staff & Know What They're Doing

The CAP and Resolution Agreement also require SEMC to conduct a self-assessment of its workforce members' knowledge and compliance with its policies and procedures, noted the Akerman attorneys. The specific policies and procedures include those that address:

- Transmitting ePHI using unauthorized networks;
- Storing ePHI on unauthorized information systems, including unsecured networks and devices;
- Removing PHI from SEMC;
- Prohibition on sharing accounts and passwords for ePHI storage and access;
- Encryption of portable devices that access or store ePHI; and
- Security incident reporting related to ePHI.

To conduct the self-assessment, SEMC must make unannounced site visits to five of its departments, interview 15 randomly selected workforce members, and inspect at least three portable devices at each of the five departments. Based on the self-assessment, SEMC must then determine if it needs to revise its HIPAA policies and procedures.

Takeaway: "Effectively educate workforce members about [your organization's] policies and procedures, including the reporting of suspected security incidents or other potential HIPAA breaches," the Akerman attorneys recommended. "Workforce members must know the organization's contact person to report suspected improper uses or disclosures of PHI."

Encrypt All Portable Devices Containing Any PHI

The other part of this settlement agreement involves a separate breach incident. In August 2014, SEMC notified OCR of a breach incident involving unsecured ePHI stored on a former employee's personal laptop and a USB flash drive. The breach affected 595 individuals.

Another important lesson from this case is that you must "encrypt all laptops or portable devices with any PHI," Sheldon-Dean stressed.

Best bet: "Implement robust policies addressing the use of portable devices, including encryption requirements and 'wiping' technology," the Akerman attorneys advised. Also, respond to suspected security incidents in a timely manner, "including mitigating the harm from such incidents and documenting how the incident was addressed."

Lesson learned: You may want to take this Resolution Agreement to heart and use it in your HIPAA training and compliance preparations. Conduct your own self-assessment to determine the effectiveness of your organization's HIPAA policies and training, the Akerman attorneys suggested. "This settlement shows that it is not enough to have the required policies. Rather, your workforce members must also understand and follow them.

You can read the SEMC Resolution Agreement at www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/SEMC/semc.html.